(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－294325

(43)公開日　平成10年(1998)11月４日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０１Ｌ　21/60	３０１	Ｈ０１Ｌ　21/60	３０１Ａ

審査請求　未請求　請求項の数18　ＯＬ　外国語出願　（全 42 頁）

(21)出願番号　特願平10－82375

(22)出願日　平成10年(1998)２月24日

(31)優先権主張番号　８０４７９２

(32)優先日　1997年２月24日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　598045380
ジェネラル・インスツルメント・コーポレイション
アメリカ合衆国ペンシルベニア州ホースハム，トーナメント・ドライブ　101

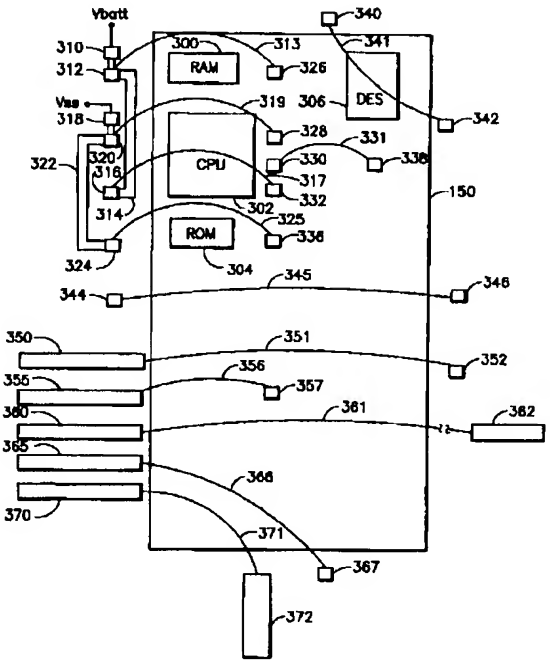
(72)発明者　プラント・キャンデロア
アメリカ合衆国カリフォルニア州サンディエゴ，フェルスパー・ストリート　2244

(74)代理人　弁理士　竹内　澄夫　（外１名）

最終頁に続く

(54)【発明の名称】　集積回路用いじり回し防止ボンドワイヤ

(57)【要約】
【課題】海賊によるICチップのプロービングを妨げまたは邪魔する装置を与える。
【解決手段】集積回路(IC)用のいじり回し防止シールドは，ICのエポキシ封止層のような保護層を通過するボンドワイヤを有する。該ボンドワイヤは，保護プロセッサのようなICの能動コンポーネントを機能させる定常状態電流のような信号を運ぶ。当該ボンドワイヤは封止層の内部及び／または付近に保持され，その結果ICのデキャプシュレーションが導電部材の破れを生じさせ，それによってプロセッサが非機能状態になる。当該ボンドワイヤは，内部または外部ボンドパッドの使用，リードフレームコンタクトの使用を含むさまざまな構成でプロセッサへ，及び／またはICが保持されるコンピュータボードへ直接的に接続され得る。金属シールド層は能動コンポーネントと封止層のトップ部分との間に配置され，海賊が能動コンポーネント領域を探知するべく電子マイクロスコープを使用することを妨げる。



【特許請求の範囲】
【請求項１】集積回路(IC)の能動コンポーネントをプロービングから保護するためのいじり回し防止装置であって，前記能動コンポーネントを機能させるための信号を運ぶよう取り付けられたワイヤから成り，前記ワイヤは，前記能動コンポーネントが機能している時にそれへのアクセスを妨害するよう，少なくとも部分的に前記能動コンポーネント上にわたって伸長する，ところの装置。
【請求項２】請求項１に記載の装置であって，前記ワイヤは第１ターミナスと第２ターミナスとの間に伸長し，前記第１ターミナスは前記プロセッサの外部にあり，前記第２ターミナスは前記プロセッサの内部にある，ところの装置。
【請求項３】請求項１に記載の装置であって，前記ワイヤは第１ターミナスと第２ターミナスとの間に伸長し，前記第１及び第２ターミナスは両方とも前記プロセッサの外部にある，ところの装置。
【請求項４】請求項１に記載の装置であって，前記ワイヤは第１ターミナスと第２ターミナスとの間に伸長し，前記第１及び第２ターミナスは両方とも前記プロセッサの内部にある，ところの装置。
【請求項５】請求項１から４のいずれかに記載の装置であって，前記ワイヤがグリッドパターンを形成する，ところの装置。
【請求項６】請求項１から５のいずれかに記載の装置であって，前記ワイヤは少なくとも部分的に前記ICの保護層内に保持され，その結果前記ワイヤは前記保護層が除去される時に破れるように取り付けられている，ところの装置。
【請求項７】請求項１から６のいずれかに記載の装置であって，さらに前記能動回路の少なくとも一部分をシールドする金属シールド層，を含む装置。
【請求項８】請求項１から７のいずれかに記載の装置であって，さらに前記ICはスマートカード内に埋め込まれ，前記ワイヤは，前記ICが前記スマートカードから除去されるときに破れるように取り付けられている，ところの装置。
【請求項９】集積回路(IC)の能動コンポーネントをプロービングから保護するためのいじり回し防止装置であって，前記能動コンポーネントを機能させる信号を運ぶよう取り付けられた導電エポキシ部材から成り，前記導電エポキシ部材は，前記能動コンポーネントが機能している時にそれへのアクセスを妨害するよう，少なくとも部分的に前記能動コンポーネント上にわたって伸長する，ところの装置。
【請求項１０】請求項９に記載の装置であって，前記導電エポキシ部材は，少なくとも部分的に前記能動コンポーネント上にプリントされる，ところの装置。
【請求項１１】請求項９または１０に記載の装置であって，前記ICはスマートカード内に埋め込まれ，前記導電エポキシ部材は，前記ICが前記スマートカードから除去される際に破れるように取り付けられている，ところの装置。
【請求項１２】請求項９から１１のいずれかに記載の装置であって，前記導電エポキシ部材は第１ターミナスと第２ターミナスとの間に伸長し，前記第１ターミナスは前記プロセッサの外部にあり，前記第２ターミナスは前記プロセッサの内部にある，ところの装置。
【請求項１３】請求項９から１１のいずれかに記載の装置であって，前記導電エポキシ部材は第１ターミナスと第２ターミナスとの間に伸長し，前記第１及び第２ターミナスは両方とも前記プロセッサの外部にある，ところの装置。
【請求項１４】請求項９から１１のいずれかに記載の装置であって，前記導電エポキシ部材は第１ターミナスと第２ターミナスとの間に伸長し，前記第１及び第２ターミナスは両方とも前記プロセッサの内部にある，ところの装置。
【請求項１５】請求項９から１４のいずれかに記載の装置であって，前記導電エポキシ部材は少なくとも部分的に前記ICの保護層内に保持され，その結果前記導電エポキシ部材は前記保護層が除去される際に破れるように取り付けられている，ところの装置。
【請求項１６】請求項９から１５のいずれかに記載の装置であって，さらに前記能動回路の少なくとも一部分をシールドする金属シールド層，を含む装置。
【請求項１７】集積回路(IC)の能動コンポーネントをプロービングから保護するためのいじり回し防止装置であって，前記能動コンポーネントへのアクセスを妨害するべく前記能動コンポーネント上にわたって少なくとも部分的に伸長するワイヤ構造物，から成る装置。
【請求項１８】請求項１７に記載の装置であって，前記ワイヤ構造物はグリッドパターンを形成する，ところの装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は集積回路の保護に関し，特にICのリバースエンジニアリングを妨げる方法に関する。本願は，不許可ユーザーがテレビ放送を受信できないようにケーブル及び衛星テレビデコーダ内で使用される安全ICを保護する際に特に有用である。本願は同時に，電子貯金の送信手続き用のスマートカード，ターミナル，アクセス制御，電子ゲーム等を含むその他の応用において使用される安全ICを保護する際に有用である。
【０００２】
【従来の技術】ペイテレビジョン市場の人気が持続することによって，“海賊”と呼ばれる不許可の人々にとって，必要な契約料を支払わずにテレビ番組を受信できる

ようにセットトップボックス（例えば，デコーダ）のアクセス制御を修正するようなすさまじい金銭的モチベーションが存在する。修正されたデコーダはさまざまな市場を通じて不謹慎な個人によって購入され，テレビ信号を不法に受信しかつ視聴するのに使用される。

【０００３】修正デコーダを製造するために，海賊は，通常は許可された製造者にのみ知られる純粋なデコーダからある情報を引き出さなければならない。典型的に，該デコーダは，スクランブルされたテレビ信号または他の番組サービス信号（例えば，オーディオまたはデータ）をデスクランブルする際に使用される暗号キーのような情報を含む安全（例えば，暗号）プロセッサを有する。該安全プロセッサはアクセス制御機能として働くため，そこに海賊の注意が集中する。したがって，海賊は，安全プロセッサから情報を得ようとしてさまざまなテクニックを使う。

【０００４】ひとつの通常の攻撃テクニックは“プロービング”として知られている。安全プロセッサは，半導体材料のモノリシックブロック内部で相互接続されたトランジスタ，抵抗，容量，及びダイオードを含む能動及び受動素子のアンサンブルによって，モノリシックデバイスとして組み立てられた集積回路を有する。プロービングの間，超大規模集積回路(VLSI)のようなICは，ダイ（例えば，ICまたは“チップ”）がデキャプシュレーション(decapsulation)により露出されるところの侵入攻撃を受けやすい。デキャプシュレーション中に，ダイを包囲し封止する化合物材料が規則的に除去される。その後，電流及びその他のパラメータを測定するプローブが使用され，チップの能動コンポーネント内の電気信号がモニターされる。ここで使用される“いじり回し(tampering)”の語は，プロービング及びデキャプシュレーションの両方を意味するものである。

【０００５】海賊は以下のデキャプシュレーション工程を実行して，プロービング用にチップを準備してもよい。最初に，チップはICパッケージ内部のダイとともにデコーダボードから除去される。概して，この場合チップは大きいボード上にマウントされている。該デコーダボードはパーソナルコンピュータ(PC)内で使用されるようなコンピュータボードであってもよい。もし当該チップが，自己崩壊特性を回避するためにバッテリー等から直流電流を要求するなら，ボードから除去する前にチップの外側の正電圧ピン（例えば，V_{batt}）及び負電圧ピン（例えば，V_{ss}）へバッテリー配線が鑞付けされる。その後，当該チップはバッテリー配線が着いたままボードから除去される。もし，バッテリーパワーが遮断されると，当該チップはメモリ内に保存された決定的な情報を消去して自己崩壊し得る。海賊はバッテリーに接続されたボード上のトレースの抵抗測定をしながら適正なバッテリーピンを識別し，主電圧（例えば，V_{cc}）をオフした状態でトレースの電圧を読んで確かめる。

【０００６】二番目に，ICパッケージの封止化合物内部のダイの位置はICパッケージのX線写真によって決定される。三番目に，ダイを破壊せずにダイの表面上の封止化合物をできるだけ多く除去するためにグラインダー機械が使用される。四番目に，化学エッチングまたはプラズマエッチングが実行され，プローブされるべきダイの領域に残った最後の封止化合物が除去される。化学エッチングは封止化合物に対して非常に良く作用するため，グラインダー工程はしばしば省略される。

【０００７】アプリケーション・スペシフィック・IC(ASIC)を含む現在のチップデザインにおいて，概して海賊は上記４つの工程を実行する際大きな障害には出くわさない。バッテリー配線が着いたままでチップをボードから除去するのは，通常最もデリケートな作業であると考えられている。不活性なグラシベーションコーティングによって保護されている未破壊ダイは，バッテリーパワーの短絡回路または開回路が作成されない限り，海賊によって露出されてしまう。さらにまた，ボンドワイヤへのダメージも容易に避けられる。以下に詳細に説明されるように，ボンドワイヤは保護封止パッケージ内でチップのボンドパッドをパッケージパッドに結合し，デバイスの周辺に配置される。デキャプシュレーション処理によって，決定的なボンドパッドが配置されるところの，すなわちバッテリーパワーが能動素子に入力されるところの領域においてダイの露出を防止できる。

【０００８】プロービングを妨げるひとつのアプローチが，Gilbergらによって通常譲渡された米国特許第4,933,898号，1990年6月12日発行の題名"Secure Integrated Circuit Chip With Conductive Shield"に記載されている。ここでGilbergらは，ICの保護領域を覆うためのひとつまたはそれ以上の導電層を使用することを開示する。当該導電層は保護領域の検査を妨げ，パワー信号をICへ運ぶ。海賊によって層のひとつが除去されると，保護領域の素子のパワーが損失される。しかし，このアプローチの実行はいくらか複雑である。

【０００９】

【発明が解決しようとする課題】したがって，海賊によるICチップのプロービングを妨げまたは邪魔する装置を与えることが所望される。特に，ボンドワイヤが破られたときICの機能停止をもたらすよう，標準のボンドワイヤを使用するバリヤーをデキャプシュレーションに対して与えることが所望される。該バリヤーは既存のチップ設計と互換性があり，実行が廉価である。本発明は上記及び他の利点を有する装置を与える。

【００１０】

【課題を解決するための手段】本発明にしたがって，集積回路用のいじり回し防止シールドが与えられる。該シールドは，メモリ，CPU，及び他のマイクロ電子素子を含む安全プロセッサのような能動コンポーネントを保持するための基板を含むICに使用するように適用される。

該ICはプロセッサを保護するためのエポキシ封止層のような保護層を有する。

【００１１】いじり回し防止シールドは，プロセッサを機能させる信号を運ぶためのボンドワイヤのような導電部材から成る。この信号は，正及び負端子を通じてバッテリーによって供給される定常状態電流を含む。該ワイヤは少なくとも部分的にICの保護層内に保持され，その結果保護層を除去するとワイヤが破れ，それによって開回路が生じる。

【００１２】該ワイヤはさまざまな構成でプロセッサへ接続され得る。例えば，該ワイヤはプロセッサに対して外部にある第１ターミナスとプロセッサに対して内部にある第２ターミナスとの間に接続されてもよい。さらに，導電部材は，プロセッサのマイクロ電子回路に対して外部及び／または内部にある点の間に伸長してもよい。該ターミナスは例えばプロセッサ内部のボンドパッド，またはプロセッサ外部のボンドパッド若しくはリードフレームコンタクトでもよい。

【００１３】変形的に，ワイヤまたは他の導電部材は，両方ともプロセッサの外部にある第１及び第２ターミナスの間に接続されてもよい。付加的に，当該ワイヤはマイクロ電子回路の表面を横切ってもよく，及び／またはマイクロ電子回路及び／またはプロセッサから離れた領域に伸長してもよい。

【００１４】導電部材は，両者ともプロセッサの内部にある第１及び第２ターミナスの間に接続されてもよい。

【００１５】他の構成において，導電部材は，導電エポキシ，及び／またはエッチング液に対して所望の耐食性を有するように形成された物質から成ることもできる。当該導電エポキシは，トレースとしてマイクロ電子回路に対してプリントされる。この場合も，ICの保護層を除去するために海賊がエッチング液を使用すると，導電エポキシが破壊され，それによってプロセッサを機能させる信号が消滅する。

【００１６】すべての構成において，たとえ海賊が導電部材をそのままにしてダイをデキャプシュレートすることに成功したとしても，空中に伸びた導電部材は克服の困難な危険を与えるため，当該導電部材は機械的プローブまたは電子マイクロスコープを有するプロービングに対して物理的障害物となる。ダイをプローブしかつ導電部材の破壊を避けるために，海賊はプローブを連続的に持ち上げたまま異なる角度でアプローチできるように別の位置に当該プローブを再構成しなければならない。実際，導電部材はプローブ配置をさらに困難にするようグリッドパターンで形成されてもよい。

【００１７】さらにまた，海賊が例えばそこに含まれるプロセッサまたはマイクロ電子回路を見渡す（すなわち，マッピングする）のに電子マイクロスコープを使用するのを妨げるべく，該プロセッサと封止層のトップ部分との間に金属シールド層が配置されてもよい。いじり回し防止ボンドワイヤシールドとともに金属シールドを使用すると，海賊にとって更なる障害物となり，それによって海賊の仕事が時間の浪費となり高くつく。

【００１８】当該ICはスマートカード内に保持されてもよい。さらに，該スマートカードの本体部分が封止層を与えてもよい。

【００１９】付加的に，マイクロ電子素子のプロービングを妨げるべく，電気信号を運ばないワイヤが少なくとも部分的にマイクロ電子素子上に伸長してもよい。特に，該ワイヤは，海賊がプローブの先端をマイクロ電子素子付近に配置しかつ移動するのを困難にするよう，グリッドパターンを形成してもよい。

【００２０】

【発明の実施の形態】テレビデコーダ内で使用される安全プロセッサのような能動コンポーネントがいじり回されないように（例えば，リバースエンジニアリングされないように），集積回路用のいじり回し防止(anti-tamper)装置が与えられる。

【００２１】図１は，デキャプシュレートされた集積回路の単純化された図である。集積回路100はエポキシ封止化合物領域110を含む。多くのパッケージピンPがリードワイヤWを通じてそれぞれのボンドパッドBへ接続されている。ボンドパッドまたはダイパッドはダイ130の周辺に備わっている多くの金属結合ピンのひとつであって，特定の回路部分（例えば，入力／出力(I/O)ポート）を対応する外部パッケージピンと接続するのに使用される。該パッドのピッチは，隣接するI/OボンドパッドBの中間点の間の距離（例えば，ミクロン）である。ダイは，例えば，マイクロ電子素子を含むシリコンマイクロチップから成る。パッケージピンP，ワイヤW及びボンドパッドBは，IC 100へ及びそこから電流を運び，普通にダイ130を覆っているエポキシ化合物が上記したデキャプシュレーティング工程を使って除去されたとき，露出される。

【００２２】ワイヤ接合は，細いワイヤがダイI/Oパッドとパッケージパッドとの間に接合されるところのダイパッケージング処理におけるひとつの工程である。例えば，ダイ130は能動コンポーネント150，152，154及び156を含む。特に，コンポーネント150は，暗号情報を含む安全プロセッサであっても良い。こうしてダイコンポーネントは，暗号情報及び能動コンポーネントの他の動作特性を突き止めるべく露出されかつプローブされる。

【００２３】図２は，本発明に従ういじり回し防止ワイヤシールドを有する集積回路の断面図である。IC 200はトップエポキシ層210及びボトムエポキシ層212を有する。ボンドワイヤ270などの導電部材がボンドパッド260及び262を連結するように示されている。該導電部材は円形断面を有する必要はないことに注意すべきである。したがって，ここで使用されている“導電部材”及び“ワイヤ”の語は円形断面を有する単一フィラメント部

材に限定されず，巻き上げられまたはよられた複数のフィラメント構成，さまざまな断面を有する構成，矩形断面を有する構成，メッシュ構成，単一のワイヤが２つ以上の端子に接続される構成，若しくは仮想的にあらゆる導電部材を包含する。特に，ワイヤは，以下に図４との関連で詳細に説明するように，プローブがメッシュを通過できないように，若しくはメッシュ内を単純に移動できないようにするのに十分な小さい間隔を有するグリッドパターンを備えることもできる。実際，当該ワイヤがプロセッサが機能するのに必要な電気信号を運ばないときでさえ，グリッド構成が使用されてもよい。ほんのグリッドの存在が，プロービングの妨害物として働く。

【００２４】さらに，導電部材270は，所望の導電率を達成するよう銀などの導体材料をエポキシにドープして形成した導電エポキシのような物質から成ることもできる。有利なことに，当該エポキシは当該ICの保護層とエッチングに対する耐食性が類似するように選択され，及び／または導電エポキシの耐食性は海賊が使用すると思われる特定のエッチング液用に仕立てられる。該導電エポキシはダイの表面に直接プリントされてもよい。

【００２５】グラシベーション層220もまた与えられる。グラシベーションとは，回路を保護するべく，完成されたダイの全表面上に載置される不活性保護コーティングを言う。グラシベーションはダイの表面を，化学及び水分汚染，ハンドリングダメージ，及び自由粒子によって引き起こされるダイのショートの可能性から守る。それはまた金属マイグレーション，及び他の金属デグラデーションを抑制する。

【００２６】シールド230は，図１のコンポーネント150～156のようなIC内部のさまざまなコンポーネントへ電流を与える金属層である。もし当該シールドへのパワーが遮られると，保護処理コンポーネントが自己崩壊し，その結果安全プロセッサ内に保存されている暗号データが消去される。付加的に，シールド230は，海賊がランダムアクセスメモリ(RAM)等の安全プロセッサの内部の変化（例えば，電圧変化）を検出するために走査電子マイクロスコープを使用することを妨げ，またシールドに被覆された部品間の区別をぼんやりとさせる。当該シールドは封止層内に配置されてもよく，それは基板250内のチップ上に配置されたひとつまたはそれ以上の保護層を含む。パッシベーション層240は，例えば，さまざまな拡散工程の間にダイの表面にわたって付着されるシリコン二酸化物から成る保護表面コートである。基板250はICがその上で組み立てられまたは組み合わされるところの物理的材料である。モノリシックICに対して，典型的に，該基板はシリコンから成る。

【００２７】議論されたように，ASICのようなチップは，たとえダイがバッテリー付勢の自己崩壊特性を有する場合でも，海賊によりデキャプシュレートされることで比較的簡単な手法でダイを露出させられる。本発明にしたがって，ボンドパッドとパッケージパッドを結合するのに使用されるタイプのボンドワイヤ270のような標準的ボンドワイヤなどのひとつまたはそれ以上の導電部材が，当該ダイを覆うように配置され，その結果いじり回し防止シールドが形成される。特に，チップの組立中に封止化合物は融解状態にあり，ダイの上に掛けられているいじり回し防止ボンドワイヤの周辺及び下方へ流れる。化合物（例えば，層210）が固体化したとき，それは，ボンドワイヤを破壊し（例えば，破って）安全プロセッサの自己崩壊を開始させる危険性によって，海賊がワイヤ埋め込み層を除去するべくグラインド機械を使用することをより困難にするような恐るべき障害物をもたらす。

【００２８】例えば，バッテリー等からの直流電流によって付勢された暗号チップの場合には，もし導電部材が破られれば，秘密データを維持するRAMへの電力がカットされ，それによってデータの消去が引き起こされる。もし導電部材がバッテリー付勢消去特性を有しないコンポーネント内で使用されれば，該導電部材は代わりにさまざまな制御信号を運んでもよい。しかし，秘密データの消去無しでそのような制御信号を運ぶ導電部材を破壊できたとしても，海賊は時間浪費的で困難な必要な補修を実行するまで，プロービングによる攻撃を妨げられる。

【００２９】さらに，たとえ海賊が導電部材を破壊することなく層210を幾分注意深く除去できたとしても，導電部材の下方のエポキシがエッチングされるときまでに，当該導電部材は侵食されかつエッチング液の腐食性によって破られる。導電部材内の金属はエポキシをエッチングするのに有用な化学的エッチング液と反応するように選択されているので，このようになる。したがって，エッチング液に対し比較的低い耐食性を有するアルミニウムのような材料を選択することが所望される。金のような他の金属はエッチング液に対し比較的高い耐食性を有する。さらに，もし導電部材がバッテリーによって付勢されれば，エッチング液はより活発に反応する。概して，導電部材材料の選択は特定のエッチング液に対する所望の耐食性を与えるべく調整される。導電エポキシがエポキシ封止層と同様のエッチング耐食性を有するように作られるとき，当該導電エポキシは特に有用である。

【００３０】図３は，本発明に従ういじり回し防止ボンドワイヤシールドを有する集積回路の安全プロセッサの平面図を略示したものである。該安全プロセッサ150は例えば，RAM 300，中央演算処理装置(CPU)302，読みとり専用メモリ(ROM)304及びデータ暗号化標準(DES)プロセッサ306を含む。しかし，本発明は，未暗号化の所有情報を守るべく保護される非安全(non-secure)プロセッサに対しても同様に応用可能である。したがって，ここで使用される“プロセッサ”の語は，暗号化プロセッ

サ，非暗号化プロセッサ，及び仮想的にあらゆるタイプのマイクロ電子回路またはマイクロ電子コンポーネントを含むことを意味する。

【００３１】図３は，ICのいじり回し防止シールド内でのボンドワイヤのような導電部材のさまざまな可能な配置を示している。図示されたすべてのボンドワイヤが必要という訳ではなく，ボンドワイヤの特定の数及び配置は変化し得ることが理解できよう。

【００３２】ひとつの構成例において，正電圧V_{batt}を有する信号がボンドパッド310へ供給され，それはボンドパッド312，トレース314，及びボンドパッド316へ電気的に接続されている。同様に，負電圧V_{ss}がボンドパッド318へ与えられ，それはボンドパッド320，トレース322，及びボンドパッド324へ電気的に接続されている。電圧V_{batt}は，途切れた時にプロセッサ150の自動消去（例えば，自己崩壊）特性を引き出す電流を与えるのに使用される。

【００３３】ボンドワイヤは，プロセッサ150の外部にあるボンドパッドと，プロセッサ150の内部にある（例えば，内部に配置された）ボンドパッドとの間に接続される。例えば，ボンドワイヤ313は外部ボンドパッド312とRAM 300の領域内の内部ボンドパッド326との間に接続されてもよい。パッド326はRAM300の外側にあるように示されているが，図示されない例えばトレースを通じて当該RAMへ電子信号を接続してもよい。

【００３４】同様に，CPU302の領域において，ボンドワイヤ319は，プロセッサ150の外部のボンドパッド320と，プロセッサ150の内部のCPU302のボンドパッド328との間に接続される。ボンドワイヤ317はプロセッサ150の外部にあるボンドパッド316とプロセッサ150の内部にあるCPUのボンドパッド332との間に接続されてもよい。ROM304の領域において，ボンドワイヤ325は外部ボンドパッド324とROM304の内部ボンドパッド336との間に接続されてもよい。

【００３５】ボンドワイヤはまた両方ともプロセッサ150内部にあるボンドパッドの間に接続されてもよい。例えば，ボンドワイヤ331は内部ボンドパッド330と338との間に接続される。

【００３６】さらにボンドワイヤはプロセッサ150の外部にあるボンドパッド間に接続されてもよい。例えば，ボンドワイヤ341は外部ボンドパッド340と342との間に接続され，ボンドワイヤ345は外部ボンドパッド344と346との間に接続される。

【００３７】付加的に，ボンドワイヤは，リードフレームコンタクトと，外部若しくは内部ボンドパッドまたは他のリードフレームコンタクトとの間に接続され得る。例えば，ボンドワイヤ351はリードフレームコンタクト350と外部ボンドパッド352との間に接続されてもよい。ボンドワイヤ356はリードフレームコンタクト355と内部ボンドパッド357との間に接続されてもよい。ボンドワイヤ361はリードフレームコンタクト360と他のリードフレームコンタクト362との間に接続されてもよい。破線で示されるように，リードフレームコンタクト362は，コンタクト360よりもプロセッサ150から遠くに配置されたパッケージリードである。図３のリードフレームコンタクト及びボンドパッドの配置は，必ずしも計る必要はない。ボンドワイヤ366はリードフレームコンタクト365と外部ボンドパッド367との間に接続されてもよい。ボンドワイヤ371はリードフレームコンタクト370と他のリードフレームコンタクト372との間に接続されてもよい。

【００３８】さらにまた，ボンドワイヤは，ボンドパッド若しくはプロセッサ150のリードフレームコンタクトと該プロセッサ150が載置されるところのデコーダボード（例えば，パーソナルコンピュータボード）とを直接接続し，またはボンドワイヤがプロセッサ150によって使用するための他の信号若しくは電流ループを運ぶことができるようなあらゆる他の配置で接続される。この場合，ボードまたは他の位置からチップパッケージを除去するだけで，いじり回し防止ボンドワイヤが破損する。

【００３９】付加的に，ボンドワイヤは，当該ボンドワイヤがプロセッサ150の表面にわたって伸長するのではなく，例えばループとして（図示せず）該プロセッサの表面から離れて伸長するように，外部パッド340と342との間に接続される。同様の構成がコンタクト370及び372にも実行され，そこではボンドワイヤ371がプロセッサ150から離れて伸長する。したがって，ボンドワイヤは，海賊が発見できないようなプロセッサ150から幾分離れた領域を通ることができる。

【００４０】安全プロセッサ150はスマートカード内に埋め込まれたIC内に保持されてもよい。典型的に，当該スマートカードはICを含むプラスチック製のクレジットカードほどのサイズのものである。当該スマートカードがリーダー内に挿入されると，コンポーネントがICとインターフェースすることができる。ICをカード内にパッケージするさまざまな方法が存在する。例えば，ICがリードフレームのコンタクトとワイヤ接合された後，エポキシがカードの射出成形の前にダイの周りにトランスファー成形される。他の方法として，コンタクト／ダイ組立体をスマートカード本体に挿入する前に，同一のカード本体内の穴にエポキシを適用する方法がある。いずれの場合でも，エポキシ封止化合物は導電部材の周りに流される。

【００４１】さらにまた，スマートカード本体はICの封止層の部分を形成する。さらに，ICのボンドワイヤはICが埋め込まれた領域から離れたスマートカード本体内を通過し，その結果スマートカードをいじるとボンドワイヤが破られる。

【００４２】スマートカード内でのいじり回し防止シールドを与えるための導電エポキシの使用は，カードに対

してより薄いプロファイルをもたらすために特に有利である。該導電エポキシはIC上を伸長する細いトレースとしてプリントされる。

【００４３】図４は本発明に従うプロービング防止ワイヤグリッドシールドを有する集積回路の安全プロセッサの平面図である。ボンドワイヤは，プローブ先端がメッシュを通過し若しくはメッシュ内を容易に移動することを妨げるのに十分に小さい間隔を有するグリッドパターンで与えられる。実際にこの構成は，プロセッサが機能するのに必要な電気信号をワイヤが運ばないときでさえ使用され得る。ワイヤ（例えば，ダミーワイヤ）がグリッド状に存在するだけで，プロービングの妨害物として機能する。

【００４４】ワイヤグリッドシールドの実行例において，プロセッサ450はメモリのようなマイクロ電子コンポーネント410を含む。ボンドワイヤ421，423，及び425はボンドパッド420と430，422と432，及び424と434との間にそれぞれ接続される。同様に，ボンドワイヤ451，453，及び454はボンドパッド448と460，452と462，及び454と464との間にそれぞれ接続される。当該ワイヤはグリッドパターン460を形成し，マイクロ電子コンポーネント410を覆う。グリッド460の寸法は，海賊が使用するプローブの先端の移動を困難にするように調節される。

【００４５】付加的に，グリッド460のワイヤはマイクロ電子回路410によって使用される作動信号を運んでもよい。この場合，短絡回路を避けるべく互いに接触を避けることは，いくつかのまたはすべてのワイヤに対して好適である。もしそうならば，ワイヤは短絡回路を避けながらグリッドパターンを維持するのに必要なだけ互いに遠ざけられる。

【００４６】ダミーワイヤがグリッドまたは他のパターンで使用される時，エポキシまたは他のICの保護層をエッチングする際に海賊によって使用される化学的エッチング液に対する高い耐食性を有するワイヤ組成物を選択することが所望される。上記したように，金のような金属はエッチング液に対し比較的高い耐食性を有する。

【００４７】したがって，チップの不許可のデキャプシュレーションを防止するべくいじり回し防止シールド内でボンドワイヤを使用するための多くの可能な構成が存在することがわかる。本発明のいじり回し防止シールドに関し，デキャプシュレーション用にグラインダー機械を使用する海賊は，そこに大量の封止化合物若しくはボンドワイヤを破る危険性を残さなければならない。実際，ボンドワイヤは，ほとんどのエポキシがワイヤの破れを避けるために除去されないまま残るように配列される。もしワイヤが破られると，チップの自己崩壊シーケンスが開始され，または必要な制御信号経路が切断され，それによって海賊には時間を浪費する困難な補修作業が要求される。

【００４８】さらに，たとえワイヤが自己崩壊シーケンスを開始せずまたは必要な制御信号を運ぶとしても，ワイヤが存在するだけでX線機械によってチップをマッピングする作業の邪魔となる。したがって，海賊がワイヤを破ったことでプロセッサが機能しなくなったのか否かがわからないように，特にグリッドパターンで，いじり回し防止シールド内に“ダミー”ボンドワイヤを与えることで妨害物がもたらされる。いずれの場合にも，海賊の仕事はもし不可能でなければ非常に困難となり，時間浪費的で高くつく。

【００４９】発明はさまざまな特定の実施例との関連で説明されてきたが，特許請求の範囲に記載された発明の思想及び態様から離れることなくさまざまな付加及び修正が可能であることは当業者の知るところである。例えば，本発明は，エポキシ封止層を有するチップに使用する点に限定されず，仮想的にあらゆるタイプの保護層を有する若しくは保護層無しのチップに使用するべく適用されてもよい。例えば，本発明は紫外線に晒されたとき消去される電気的プログラム可能ROM(EPROM)に使用することもできる。典型的に，EPROMは空気ギャップ及び透明窓によって保護されている。この場合，導電部材は単純に該空気ギャップ内に保持され，エポキシ層がなくとも海賊にとっては障害物となる。

【図面の簡単な説明】

【図１】図１は，デキャプシュレートされた集積回路を示す単純化された図である。

【図２】図２は，本発明に従ういじり回し防止ボンドワイヤシールドを有する集積回路の断面図を示す。

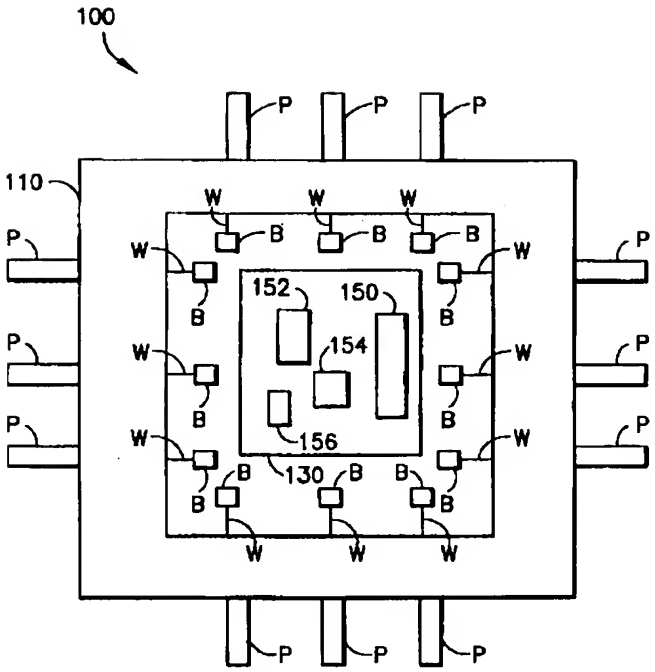
【図３】図３は，本発明に従ういじり回し防止ボンドワイヤシールドを有する集積回路の安全プロセッサの平面図である。

【図４】図４は，本発明に従うプロービング防止ワイヤグリッドシールドを有する集積回路の安全プロセッサの平面図である。

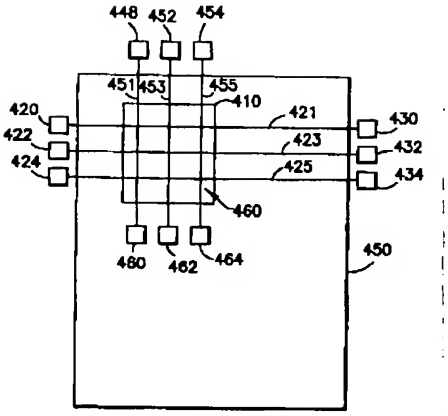
【符号の説明】

150	安全プロセッサ
300	RAM
302	CPU
304	ROM
306	DESプロセッサ
312，326	ボンドパッド
313	ボンドワイヤ
314	トレース
350	リードフレームコンタクト

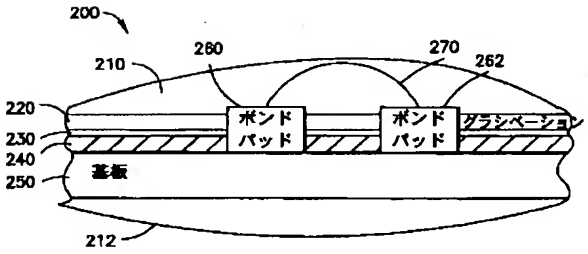
【図１】


100
110
P
W
B
152
150
154
156
130

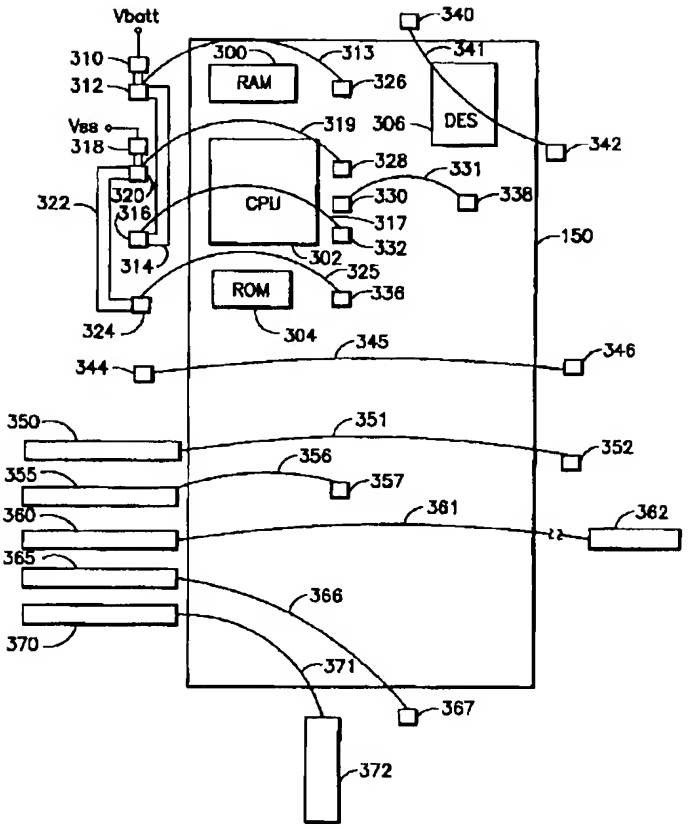
【図４】


448
452
454
451
453
455
410
420
421
430
422
423
432
424
425
434
460
450
480
462
464

【図２】


200
210
260
270
262
220
230
240
250
ボンド
パッド
ボンド
パッド
グラシベーション
基板
212

【図３】



フロントページの続き

(71)出願人　598045380
101 Tournament Drive
Horsham, Pennsylvania, The United States of America

【外国語明細書】

1.Title of Invention

ANTI-TAMPER BOND WIRE SHIELD FOR AN INTEGRATED CIRCUIT

2. Claims

1. An anti-tamper apparatus for protecting an active component of an integrated circuit (IC) from probing, said apparatus comprising:

a wire adapted to carry a signal which allows said active component to function; wherein:

said wire extends, at least in part, over said active component to hinder access thereto when said active component is functioning.

2. The apparatus of claim 1, wherein:

said wire extends between first and second terminuses; and

said first terminus is external to said processor and said second terminus is internal to said processor.

3. The apparatus of claim 1, wherein:

said wire extends between first and second terminuses; and

said first and second terminuses are both external to said processor.

4. The apparatus of claim 1, wherein:

said wire extends between first and second terminuses; and

said first and second terminuses are both internal to said processor.

5. The apparatus of one of the preceding claims, wherein:

said wire forms a grid pattern.

6. The apparatus of one of the preceding claims, wherein:

said wire is carried, at least in part, within a protective layer of said IC such that said wire is adapted to rupture when said protective layer is removed.

7. The apparatus of one of the preceding claims, further comprising:

a metallic shield layer which shields at least a portion of said active circuit.

8. The apparatus of one of the preceding claims, wherein:

said IC is embedded in a smart card; and

said wire is adapted to rupture when said IC is removed from said smart card.

9. An anti-tamper apparatus for protecting an active component of an integrated circuit (IC) from probing, said apparatus comprising:

a conductive epoxy member adapted to carry a signal which allows said active component to function; wherein:

said conductive epoxy member extends, at least in part, over said active component to hinder access thereto when said active component is functioning.

10. The apparatus of claim 9, wherein:

said conductive epoxy member is printed, at least in part, on said active component.

11. The apparatus of claim 9 or 10, wherein:

said IC is embedded in a smart card; and

said conductive epoxy member is adapted to rupture when said IC is removed from said smart card.

12. The apparatus of one of claims 9 to 11, wherein:

said conductive epoxy member extends between first and second terminuses; and

said first terminus is external to said processor and said second terminus is internal to said processor.

13. The apparatus of one of claims 9 to 11, wherein:

said conductive epoxy member extends between first and second terminuses; and

said first and second terminuses are both external to said processor.

14. The apparatus of one of claims 9 to 11, wherein:

said conductive epoxy member extends between first and second terminuses; and

said first and second terminuses are both internal to said processor.

15. The apparatus of one of claims 9 to 14, wherein:

said conductive epoxy member is carried, at least in part, within a protective layer of said IC such that said conductive epoxy member is adapted to rupture when said protective layer is removed.

16. The apparatus of one of claims 9 to 15, further comprising:

a metallic shield layer which shields at least a portion of said active circuit.

17. An anti-tamper apparatus for protecting an active component of an integrated circuit (IC) from probing, said apparatus comprising:

a wire structure which extends, at least in part, over said active component to hinder access thereto.

18. The apparatus of claim 17, wherein:

said wire structure forms a grid pattern.

3.Detailed Description of Invention

BACKGROUND OF THE INVENTION

The present invention relates to the protection of integrated circuits (ICs), and more particularly, to a scheme for preventing the reverse engineering of ICs. The invention is particularly useful in protecting secure ICs which are used in cable and satellite television decoders to prevent unauthorized users from receiving television broadcasts. The invention is equally useful in protecting secure ICs used in other applications, including terminals and smart cards for electronic funds transactions, premises access control, electronic games, and the like.

Due to the continuing popularity of the pay television market, there exists a tremendous financial motivation for unauthorized persons known as "pirates" to modify the access control of set-top boxes (e.g., decoders) to allow the reception of television programming without payment of the required subscription fees. The modified decoders are purchased by unscrupulous individuals through various markets and used to illegally receive and view the television signals.

To produce a modified decoder, a pirate must extract certain information from a genuine decoder which is usually known only to the authorized manufacturer. The decoder typically includes a

secure (e.g., cryptographic) processor which contains information such as cryptographic keys which are used in descrambling a scrambled television signal or other programming service signal (e.g., audio or data). Since the secure processor performs access control functions, it is a focal point of the pirate's attention. Accordingly, the pirate will employ various techniques in an attempt to gain information from the secure processor.

One common attack technique is known as "probing." A secure processor includes an integrated circuit (IC) which is fabricated as a monolithic device with an ensemble of active and passive components, including transistors, resistors, capacitors, and diodes which are interconnected within a monolithic block of semiconductor material. During probing, ICs such as very large scale integrated (VLSI) circuits are subject to an invasive attack wherein the die (e.g., IC or "chip") is exposed by decapsulation. During decapsulation, the compound material which encapsulates or surrounds the die is systematically removed. Then, probes which measure current and other parameters are used to monitor the electronic signals in the active components of the chip. The term "tampering" as used herein is meant to encompass both probing and decapsulation.

A pirate may perform the following decapsulation steps to prepare a chip for probing. First, the chip is removed from the decoder board, with the die still inside the IC package. Generally, this is the case when a chip is mounted on a large board. The decoder board may be a computer board such as those used in a personal computer (PC). If the chip requires a direct current from a battery or the like to circumvent a self-destruct feature, then battery wires are soldered to a positive voltage pin (e.g., V_{batt}) pin and to a negative voltage pin (e.g., V_{ss}) on the outside of the chip prior to removal from the board. The chip is then removed from the board with the battery wires still attached. If the battery power is interrupted, the chip may self-destruct by erasing critical information stored in memory. The pirate can identify the appropriate battery pins by taking resistance measurements of the traces on the board which are connected to the battery, and then confirming by taking voltage readings of the traces with a main voltage (e.g., V_{cc}) off.

Second, the location of the die within the encapsulating compound of the IC package can be determined by taking an x-ray of the IC package. Third, a mechanical grinder can be used to remove as much of the encapsulating compound as possible above the top surface of the die without damaging the die.

Fourth, chemical etching or plasma etching is performed to remove the last portions of encapsulating compound which remain over the area of the die which is to be probed. Some chemical etchants work so well on the encapsulating compound that the grinding step can often be skipped.

In current chip designs, including those for application specific ICs (ASICs), a pirate will generally not encounter significant obstacles in performing the four steps above. Removal of the chip from the board with the battery wires still attached is usually considered to be the most delicate operation. Thus, the undamaged die, which is protected by an inert glassivation coating, can be exposed by a pirate as long as a short circuit or open circuit of the battery power is not created. Furthermore, damage to bond wires can also easily be avoided. Bond wires may connect bond pads of the chip to package pads in the protective encapsulating package, and are located on the periphery of the device, as will be discussed in greater detail below. The decapsulation process can avoid exposing the die in the area where critical bond pads are located, that is, where the battery power is input into the active component.

One approach to deterring probing is discussed in commonly-assigned U.S. Patent 4,933,898, issued June 12, 1990 to Gilberg et al., entitled "Secure

Integrated Circuit Chip With Conductive Shield." Gilberg et al. disclose using one or more conductive layers to overlay a secure area of an IC. The conductive layers shield the secure area from inspection and carry a power signal to the IC. Removal of one of the layers by a pirate causes the loss of power to the components of the secure area. However, the implementation of this approach is somewhat complex.

Accordingly, it would be desirable to provide an apparatus which deters or otherwise hinders probing of an IC chip by a pirate. In particular, it would be desirable to provide a barrier to decapsulation which uses standard bond wires to render the IC non-functional when the bond wire is ruptured. The barrier should be compatible with existing chip designs and inexpensive to implement. The present invention provides a system having the above and other advantages.

SUMMARY OF THE INVENTION

In accordance with the present invention, an anti-tamper shield for an integrated circuit (IC) is presented. The shield is adapted for use with an IC which includes a substrate for carrying an active component, such as a secure processor which may include a memory, CPU, and other micro-electronic components. The IC may have a protective layer such as an epoxy encapsulating layer for protecting the processor.

The anti-tamper shield comprises an electrically conductive member such as a bond wire for carrying a signal which allows the processor to function. This signal may include a steady state electrical current which is supplied by a battery via positive and negative terminals. The wire may be carried, at least in part, in a protective layer of the IC such that removal of the protective layer will rupture the wire, thereby causing an open circuit.

The wire may be coupled to the processor in a variety of configurations. For example, the wire may be coupled between a first terminus which is external to the processor and a second terminus which is internal to the processor. Furthermore, the electrically conductive member may extend between points which are external and/or internal to

the micro-electronic circuits of the processor. The terminus may be a bond pad within the processor, or a bond pad or lead frame contact outside the processor, for example.

Alternatively, the wire or other electrically conductive member may be coupled between first and second terminuses, both of which are external to the processor. The wire may optionally traverse the top surface of the micro-electronic circuit, and/or may extend in a region away from the micro electronic circuit and/or processor.

The electrically conductive member may be coupled between first and second terminuses, both of which are internal to the processor.

In another configuration, the electrically conductive member may comprise conductive epoxy, and/or a substance which is tailored to have a desired resistance to an etchant. The conductive epoxy may be printed as a trace over the micro-electronic circuit. In this case, the use of an etchant by a pirate to remove the protective layer of the IC will also destroy the conductive epoxy, thereby terminating the signal which allows the processor to function.

In all configurations, even if a pirate was successful in decapsulating the die with the conductive members intact, the conductive member would pose a physical obstacle to probing with

mechanical probes or an electron microscope since a conductive member suspended in space present a hazard that is difficult to overcome. Probes must be continually lifted and reconfigured into new positions by the pirate to allow different angles of approach in order to probe a die and avoid rupturing any of the conductive members. In fact, the electrically conductive member may be formed in a grid pattern to further aggravate probe positioning.

Furthermore, a metallic shield layer may be disposed between the processor and the top portion of the encapsulating layer to prevent a pirate from using an electron microscope, for example, to survey (i.e., map) the processor or the micro-electronic circuits contained therein. The use of a metallic shield in conjunction with the anti-tamper bond-wire shield poses an additional obstacle to the pirate, thereby making the pirate's task more time-consuming and expensive.

The IC may be carried in a smart card. Moreover, a portion of the body of the smart card may provide the encapsulating layer.

Optionally, a wire which does not carry an electrical signal may extend, at least in part, over the micro-electronic component to deter probing of the micro-electronic component. In particular, the wire may form a grid pattern which makes it

difficult for a pirate to position and move a probe tip near the micro-electronic component.

DETAILED DESCRIPTION OF THE INVENTION

An anti-tamper apparatus for an integrated circuit (IC) is presented for preventing active components, such as a secure processor used in a television decoder, from being tampered with (e.g., reversed engineered).

FIGURE 1 is a simplified diagram of a decapsulated integrated circuit. The integrated circuit (IC), shown generally at 100, includes an epoxy encapsulating compound region 110. A number of package pins P are connected to respective bond pads B via lead wires W. A bond pad or die pad is one of many metal connection pins that reside in the periphery of the die 130, and are used to couple a unique circuit portion (e.g., input/output (I/O) port) with a corresponding external package pin. The pad pitch is the distance (e.g., in microns) between the midpoints of the adjacent I/O bond pads B. The die can comprise, for example, a silicon micro-chip which contains micro-electronic devices. The package pins P, wires W and bond pads B carry current to and from the IC 100, and are exposed when the epoxy compound which normally covers the die 130 is removed using the decapsulating steps discussed previously.

Wirebond is a step in the die packaging process where thin wires are bonded between the die I/O pads

and the package pads. The die 130 includes exemplary active components 150, 152, 154 and 156. In particular, component 150 may be a secure processor which includes cryptographic information. Thus, the die components are exposed and can be probed by a pirate to ascertain the cryptographic information and other operating characteristics of the active components.

FIGURE 2 is a cross-sectional view of an integrated circuit with an anti-tamper bond wire shield in accordance with the present invention. The IC, shown generally at 200, includes a top epoxy layer 210 and a bottom epoxy layer 212. An electrically conductive member such as a bond wire 270 is shown coupling bond pads 260 and 262. Note that the electrically conductive member need not have a circular cross-section. Thus, it should be understood that the terms "electrically conductive member" and "wire" as used herein are not limited to a single filament member having a circular cross-section, but may encompass configurations including a number of filaments which are wound or twisted together, a configuration with a varying cross section, a configuration with a rectangular cross section, a mesh configuration, a configuration wherein a single wire is coupled to more than two terminals, or virtually any electrically conductive member. In particular, the wires may be provided in

a grid pattern with a spacing which is small enough to prevent a probe from passing through the mesh or moving easily within the mesh, as discussed below in conjunction with FIGURE 4. In fact, a grid configuration may be used even when the wire does not carry an electrical signal which the processor requires to function. The mere presence of the grid serves as a deterrent to probing.

Furthermore, the electrically conductive member 270 may comprise a substance such as conductive epoxy which is formed by doping epoxy with a conductive material such as silver to achieve a desired conductivity. Advantageously, the epoxy can be selected to have a resistance to etching which is similar to the resistance of the protective layer of the IC, and/or the resistance of the conductive epoxy can be tailored according to a specific etchant which a pirate is expected to use. The conductive epoxy may be printed directly to the surface of the die.

A glassivation layer 220 is also provided. Glassivation refers to an inert protective coating which is placed over the entire surface of a completed die to protect the circuit. Glassivation protects the surface of the die from chemical and moisture contamination, handling damage, and the possibility of shorting the die caused by loose

particles. It can also inhibit metal migration and other metal degradation.

A shield 230 is a metal layer that provides current to various components within the IC 200, such as the components 150-156 of FIGURE 1. If power to the shield is interrupted, then a secure processing component may self-destruct such that cryptographic data which is stored in the secure processor is erased. Additionally, the shield 230 serves to prevent a pirate from using a scanning electron microscope to detect changes (e.g., voltage changes) in portions of the secure processor, such as a random access memory (RAM), and blurs the distinction between parts which are coated by the shield. The shield may be located within the encapsulating layer, which includes one or more protective layers which are disposed above the chip in the substrate 250. A passivation layer 240 is a protective surface coat comprising, for example, silicon dioxide which is deposited over the surface of the die during various diffusion steps. The substrate 250 is the physical material upon which the IC is fabricated or assembled. For a monolithic device, the substrate typically comprises silicon.

As discussed, a chip such as an ASIC can be decapsulated by a pirate to expose the die in a relatively straightforward manner even when the die has a battery powered self-destruct feature. In

accordance with the present invention, one or more electrically conductive members such as standard bond wires of the type used to connect a bond pad with a package pad, such as bond wire 270, are situated to cover the die such that an anti-tamper shield is formed. In particular, during fabrication of a chip, the encapsulating compound is in a molten state and flows around and below the anti-tamper bond wire which are suspended over the die. When the compound (e.g., layer 210) has solidified, it provides a formidable obstacle as it is more difficult for a pirate to use mechanical grinding equipment to remove the wire-embedded layer for fear of breaking (e.g., rupturing) the bond wires and initiating the self-destruct feature of the secure processor.

For example, in the case of a cryptographic chip powered by a direct current from a battery or the like, if the electrically conductive member is ruptured, power to a RAM which maintains the secret data will be cut, thereby causing the data to be erased. If a electrically conductive member is used in a component which did not have a battery powered erasure feature, then the electrically conductive member may instead carry various control signals. However, even the rupturing of such a control signal-carrying electrically conductive member without the erasure of secret data would thwart a

pirate's probing attack until the pirate performed the necessary time-consuming and difficult repair.

Moreover, even if a pirate could somehow carefully remove the layer 210 without rupturing the electrically conductive member, by the time the epoxy below the conductive member is etched, the conductive member may be eaten away and ruptured due to the corrosivity of the etchant. This is true since the metal in the conductive member is chosen to react to the chemical etchants which are useful in etching the epoxy. Thus, it may be desirable to choose a material such as aluminum, which has a relatively low resistance to etchants. Other metals, such as gold, have a relatively high resistance to etchants. Moreover, if a conductive member is powered by a battery, etchants will react in a more aggressive way. Generally, the selection of the conductive member material can be tailored to provide a desired resistance to particular etchants. Conductive epoxy is particularly useful as it may be formulated to have a similar resistance to etching as the epoxy encapsulating layer.

FIGURE 3 is a top view illustrating, in simplified form, a secure processor of an integrated circuit with an anti-tamper bond wire shield in accordance with the present invention. The secure processor 150, includes exemplary micro-electronic components such as a RAM 300, a central processing

unit (CPU) 302, a read-only memory (ROM) 304, and a Data Encryption Standard (DES) processor 306. However, note that the present invention is equally applicable to non-secure processors which may be protected to preserve unencrypted but proprietary information. Thus, the term "processor" as used herein is meant to encompass encrypted processors, non-encrypted processors, and virtually any type of micro-electronic circuit or micro-electronic component.

FIGURE 3 is meant to a show a variety of possible arrangements of conductive members such as bond wires in an anti-tamper shield of an IC. It should be understood that not all of the bond wires shown are required, and that the specific number and positioning of the bond wires can vary.

In one example configuration, a signal having a positive voltage V_{batt} may be supplied to a bond pad 310, which is electrically coupled to a bond pad 312, a trace 314, and a bond pad 316. Similarly, a negative voltage V_{ss} is present at a bond pad 318, which is electrically coupled to a bond pad 320, a trace 322, and a bond pad 324. The voltage V_{batt} may be used to provide a current which, when terminated, triggers an automatic erasure (e.g., self-destruct) feature of the processor 150.

Bond wires can be coupled between bond pads which are external to the processor 150 and bond

pads which are internal (e.g., located within) the processor 150. For example, a bond wire 313 may be coupled between the external bond pad 312 and the internal bond pad 326 in the region of the RAM 300. Pad 326 is shown as being located outside the RAM 300, but may couple an electrical signal to the RAM 300 via a trace, for example, not shown.

Similarly, in the region of the CPU 302, a bond wire 319 may be coupled between the bond pad 320 which is external to the processor 150 and the bond pad 328 of the CPU 302 which is internal to the processor 150. A bond wire 317 may be coupled between the bond pad 316 which is external to the processor 150 and the bond pad 332 of the CPU which is internal to the processor 150. In the region of the ROM 304, a bond wire 325 may be coupled between the external bond pad 324 and the internal bond pad 336 of the ROM 304.

Bond wires can also be coupled between bond pads which are both internal to the processor 150. For example, a bond wire 331 may be coupled between internal bond pads 330 and 338.

Bond wires can be further be coupled between bond pads which are external to the processor 150. For example, a bond wire 341 may be coupled between external bond pads 340 and 342, and a bond wire 345 may be coupled between external bond pads 344 and 346.

Additionally, bond wires can be coupled between lead frame contacts and external or internal bond pads, or other lead frame contacts. For example, a bond wire 351 may be coupled between a lead frame contact 350 and an external bond pad 352. A bond wire 356 may be coupled between a lead frame contact 355 and an internal bond pad 357. A bond wire 361 may be coupled between a lead frame contact 360 and another lead frame contact 362. As indicated by the broken line, the lead frame contact 362 may be a package lead which is located further from the processor 150 than the contact 360. Note that the positioning of the lead frame contacts and bond pads in FIGURE 3 is not necessarily to scale. A bond wire 366 may be coupled between a lead frame contact 365 and an external bond pad 367. A bond wire 371 may be coupled between a lead frame contact 370 and another lead frame contact 372.

Furthermore, a bond wire can be coupled between a bond pad or lead frame contact of the processor 150 directly to a decoder board (e.g., personal computer (PC) board) on which the processor 150 is carried, or any other location which allows the bond wire to carry a current loop or other signal for use by the processor 150. In this case, mere removal of the chip package from the board or other location will rupture the anti-tamper bond wire.

Additionally, a bond wire can be coupled between external pads, such as pads 340 and 342, where the bond wire does not extend over the surface of the processor 150, but extends away from the surface of the processor, for example, in a loop (not shown). A similar configuration can be had with the contacts, such as contacts 370 and 372, where the bond wire 371 extends away from the processor 150. Thus, the bond wire can be routed to a region which is somewhat distant from the processor 150, e.g., where the pirate may not expect to find it.

The secure processor 150 may be carried in an IC which is embedded in a smart card. A smart card is typically a plastic credit-card sized device which contains ICs. The smart card is inserted into a reader to allow a component to interface with the ICs. There are various methods of packaging ICs into a card. For example, after an IC is wire bonded to contacts of a lead frame, epoxy can be transfer molded around the die prior to injection molding of a card. Another approach is to apply epoxy to a cavity in a card body prior to insertion of the contact/die assembly into the same smart card body. In either case, an epoxy encapsulating compound can be made to flow around the conductive members.

Furthermore, the body of the smart card forms part of the encapsulating layer of the IC. Moreover, the bond wires of the IC may be routed in the body of the smart card away from the region in which the IC is embedded such that any tampering with the smart card ruptures the bond wires.

The use of conductive epoxy to provide an anti-tamper shield in a smart card is particularly advantageous since it allows a lower profile for the card. The conductive epoxy can be printed as a thin trace which extends over the IC.

FIGURE 4 is a top view of a secure processor of an integrated circuit with an anti-probing wire grid shield in accordance with the present invention. Bond wires may be provided in a grid pattern with a spacing which is small enough to prevent a probe tip from passing through the mesh or moving easily within the mesh. In fact, this configuration may be used even when the wire does not carry an electrical signal which the processor requires to function. The mere presence of the wires (e.g., dummy wires) in a grid serves as a deterrent to probing.

In an example implementation of a wire grid shield, a processor 450 includes a micro-electronic component 410 such as a memory. Bond wires 421, 423, and 425 are coupled between bond pads 420 and 430, 422 and 432, and 424 and 434, respectively. Similarly, bond wires 451, 453, and 454 are coupled

between bond pads 448 and 460, 452 and 462, and 454 and 464, respectively. The wires form a grid pattern, shown generally at 460, which covers the micro-electronic component 410. The dimensions of the grid 460 may be adjusted to aggravate the movement of the tip of a probe which a pirate may use.

The wires of the grid 460 may optionally carry a signal which is used by the micro-electronic circuit 410 to operate. In this case, it may be preferable for some or all of the wires to avoid contacting each other to avoid a short circuit. If so, the wires may be displaced from one another as required to maintain the grid pattern while avoiding a short circuit.

When dummy wires are used in a grid or other pattern, it is desirable to select a wire composition which has a high resistance to the chemical etchants which may be used by a pirate in etching the epoxy or other protective layer of the IC. As mentioned, metals such as gold, for example, have a relatively high resistance to etchants.

Accordingly, it can be seen that there are many possible configurations for using bond wires in an anti-tamper shield to prevent an unauthorized decapsulation of a chip. With the anti-tamper shield of the present invention, a pirate employing a mechanical grinder for decapsulation would have to

leave a great deal of the encapsulating compound in place or risk rupturing the bond wires. In fact, the bond wires can be arranged such that most of the epoxy must be left undisturbed to avoid rupturing the wires. If a wire is ruptured, a self-destruct sequence of the chip may be initiated, or a required control signal path may be terminated, thereby requiring a time-consuming and difficult repair by the pirate.

Moreover, even if the wire does not initiate a self-destruct sequence or carry a required control signal, the mere presence of the wire can interfere with efforts to map the chip via an x-ray machine. Thus, the mere presence of "dummy" bond wires in an anti-tamper shield, particularly in a grid pattern, will serve as a deterrent, as the pirate may not know whether rupturing the wires will render the processor non-functional. In either case, the pirate's task is made much more difficult, time-consuming and expensive, if not impossible.

Although the invention has been described in connection with various specific embodiments, those skilled in the art will appreciate that numerous adaptations and modifications may be made thereto without departing from the spirit and scope of the invention as set forth in the claims. For example, the invention is not limited to use with chips which have an epoxy encapsulating layer, but may be

adapted for use with a chip which has virtually any type of protective layer, or even no protective layer. For instance, the invention may be used with a device such as an electrically programmable read-only memory (EPROM), which can be erased when exposed to ultraviolet light. An EPROM is typically protected by an air gap and a transparent window. In this case, the electrically conductive member may be carried simply in the air gap, and will pose an obstacle to a pirate even without the epoxy layer.

4.Brief Descriprion of Drawings

FIGURE 1 is a simplified diagram illustrating a decapsulated integrated circuit.

FIGURE 2 is a cross-sectional view illustrating an integrated circuit with an anti-tamper bond wire shield in accordance with the present invention.

FIGURE 3 is a top view of a secure processor of an integrated circuit with an anti-tamper bond wire shield in accordance with the present invention.

FIGURE 4 is a top view of a secure processor of an integrated circuit with an anti-probing wire grid shield in accordance with the present invention.

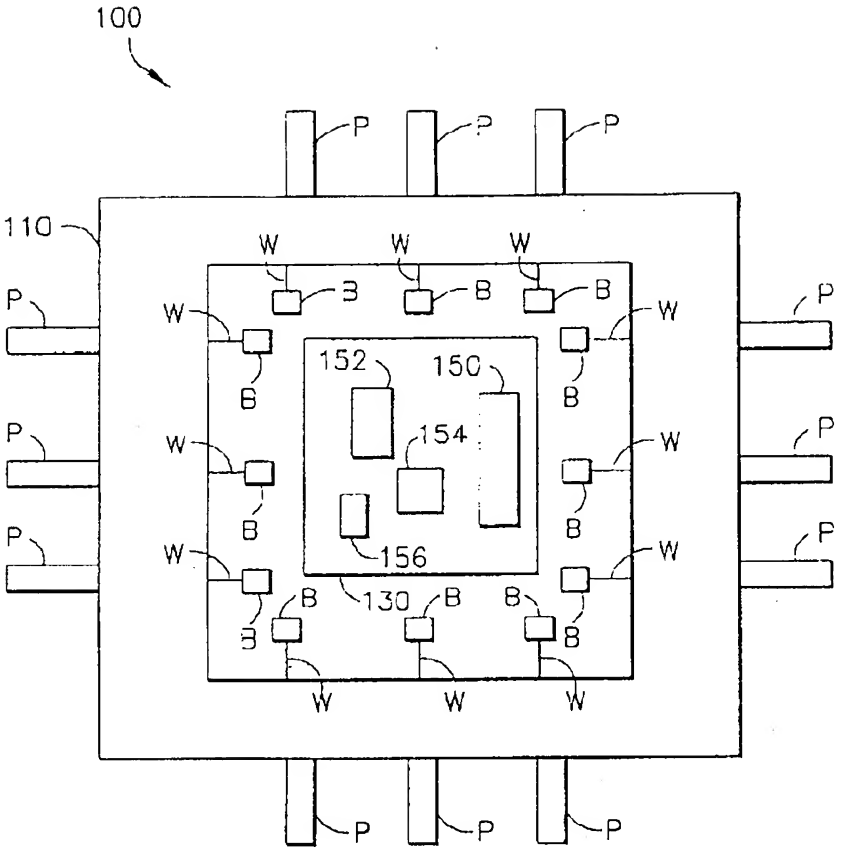


FIG.1

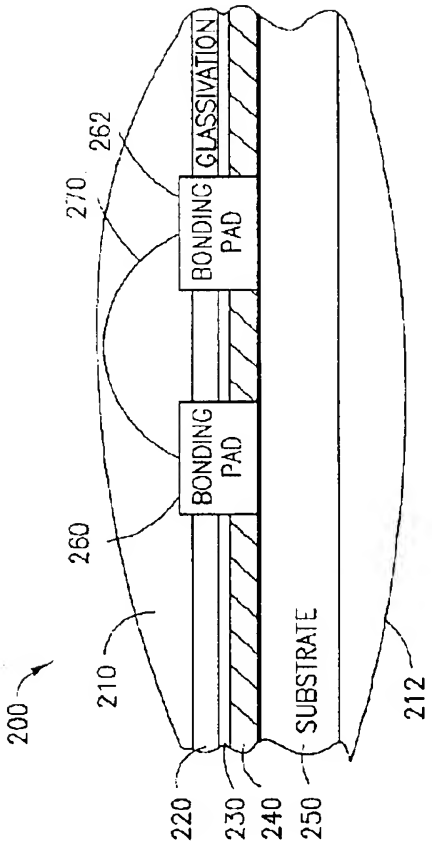

200
210
212
220
230
240
250
260
262
270
GLASSIVATION
BONDING PAD
BONDING PAD
SUBSTRATE

FIG.2

3/4

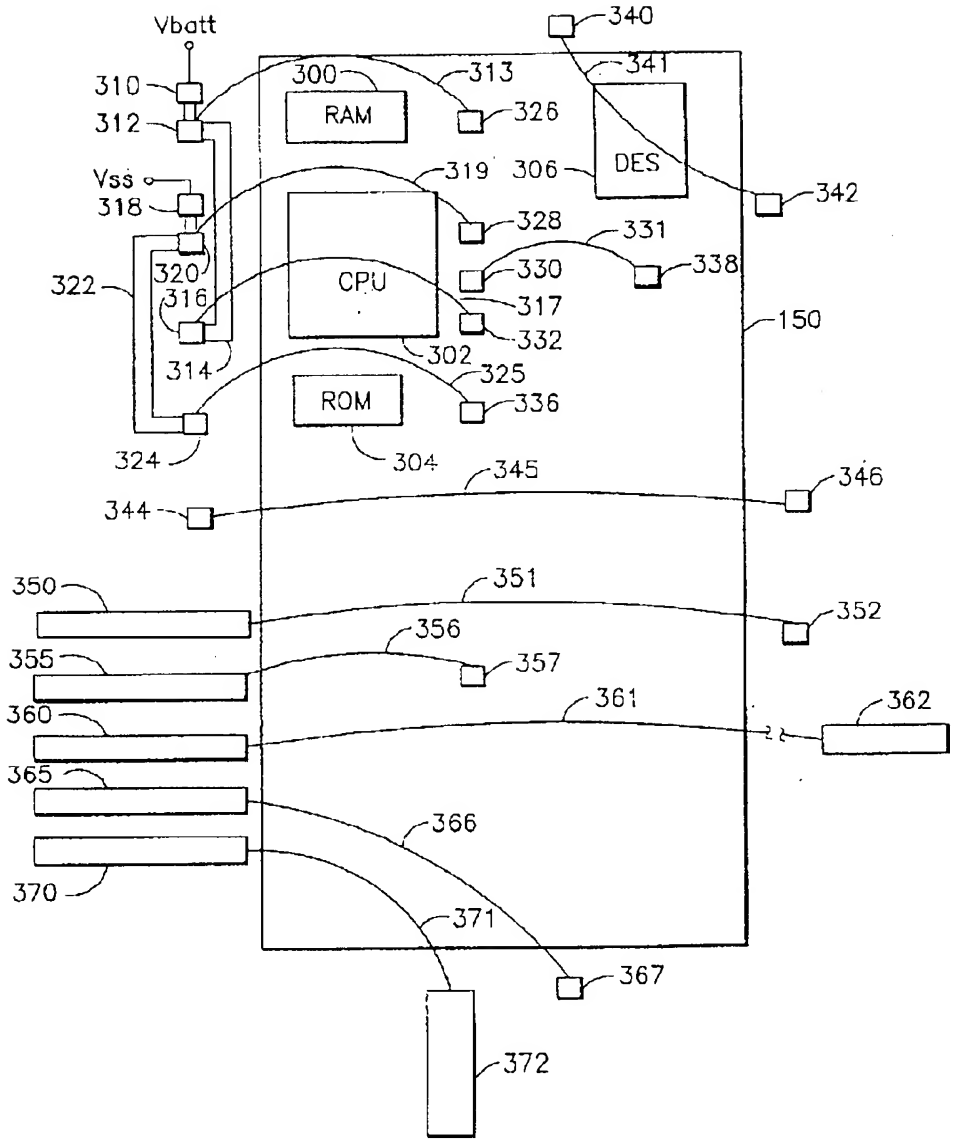

Vbatt
310
312
Vss
318
320
316
322
314
324
300
RAM
313
326
340
341
DES
306
342
319
328
331
330
338
CPU
317
332
150
302
325
ROM
336
304
345
346
344
350
351
352
356
355
357
361
362
360
365
366
370
371
367
372

FIG.3

4/4

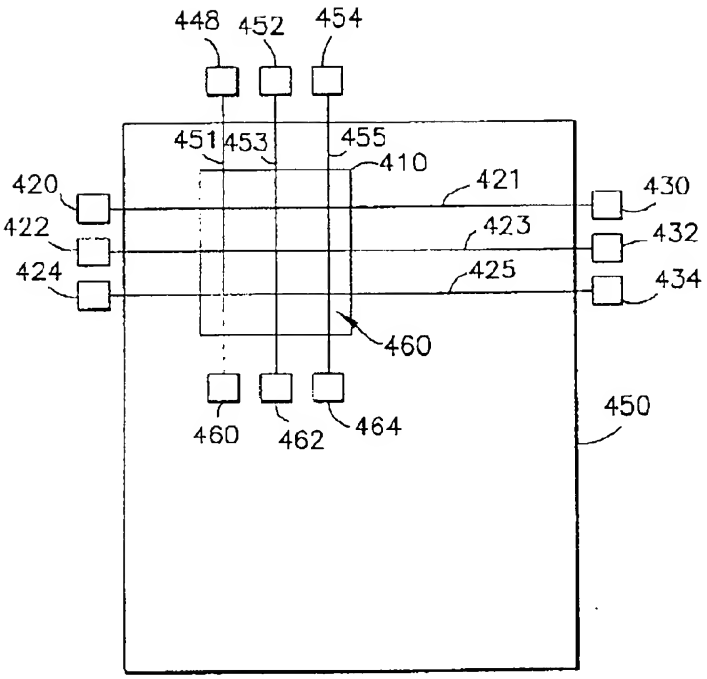

448
452
454
451
453
455
410
420
421
430
422
423
432
424
425
434
460
460
462
464
450

FIG.4

1.Abstract

An anti-tamper shield for an integrated circuit (IC) includes a bond wire which passes through a protective layer such as an epoxy encapsulating layer of the IC. The bond wire carries a signal, such as a steady state current, which allows an active component of the IC, such as a secure processor, to function. The bond wire is carried within and/or proximate to the encapsulating layer such that a decapsulation of the IC will cause a rupture of the electrically conductive member, thereby rendering the processor non-functional. The bond wire may be coupled to the processor in a variety of configurations, including the use of internal or external bond pads, lead frame contacts, and/or directly to a computer board on which the IC is carried. A metallic shield layer may be located between the active component and a top portion of the encapsulating layer to prevent a pirate from using an electron microscope, for example, to survey the active component region.

2.Representative Drawing

None